IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Mikko NEVALAINEN	Confirmation No.: 7062
Application No.: 10/599,947	Examiner: Georgewill, Opiribo
Filed: February 26, 2007	Group Art Unit: 2617

For: METHOD AND DEVICE FOR RESTRICTED EXECUTION OF
            APPLICATIONS ON A MOBILE TERMINAL

Commissioner for Patents
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated December 15,

2010.

I.   REAL PARTY IN INTEREST

The real party in interest is Nokia Corporation.

II.   RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

III.   STATUS OF THE CLAIMS

Claims 1-5, 7-16, 18-20 and 22-43 are pending in the present Application. Claims 6, 17

and 21 have been canceled, claim 12 is original claims, and claims 1-5, 7-11, 13-16, 18-20 and

22-43 are previously presented.

Claims 1-5, 7-16, 18-20 and 22-43 were finally rejected in an Office Action dated

September 15, 2010. This appeal is therefore taken from the final rejection of claims 1-5, 7-16,

18-20 and 22-43 on September 15, 2010.

IV.   STATUS OF AMENDMENTS

No Amendment has been filed subsequent to the issuance of the Final Office Action on

September 15, 2010, and all prior amendments have been entered.

V.   SUMMARY OF THE CLAIMED SUBJECT MATTER

The claimed invention addresses drawbacks associated with present technologies for

providing software (e.g., gaming software applications) to a mobile device of a user, on a trial

basis, without providing any alternatives short of requiring the user to purchase the software.

Independent claim 1 recites:

1. Method comprising:

detecting, at a mobile terminal device, an input directed to start execution of an application on

said mobile terminal device; (*See, e.g.*, Specification ¶¶ [0014], [0085])

initiating a message to a surveillance center, wherein said message indicates that the

application has been started; (*See, e.g.*, Specification ¶¶ [0015], [0086], [0121-0124])

starting a restricted execution of said application, within a predetermined functional limit,

after said message has been initiated; (*See, e.g.*, Specification ¶¶ [0016], [0088], [0121])

determining whether the message has been sent; and (*See, e.g.*, Specification ¶¶ [0045-0049],

[0052], [0087], [0125-0126])

further restricting the execution of said application, within a more restrictive functional limit,

based on said determination. *(See, e.g.,* Specification ¶¶ [0050-0053], [0127])

Independent claim 27 recites:

27. Method comprising:

receiving a message from a mobile terminal device at a surveillance center, said message

comprising application execution related data, wherein the message indicates that the

application has been started, and wherein the message is initiated after a predetermined

period of time has passed since the application was first started or after a predetermined

number of input actions has been input to the application; *(See, e.g.,* Specification ¶¶

[0012], [0015], [0019], [0026], [0030-0032], [0072], [0086], [0093])

generating, at the surveillance center, an authorization to a restricted execution of said

application within predetermined functional limits on said mobile terminal device; and

(See, e.g., Specification ¶¶ [0026], [0058], [0072], [0075], [0093], [0101])

determining to send said authorization to said mobile terminal device. *(See, e.g.,*

Specification ¶¶ [0026], [0058], [0072], [0094], [0101])

Independent claim 32 recites:

32. An apparatus comprising:

at least one processor; and

at least one memory including computer program code,

the at least one program code configured to, with the at least one processor, cause the

apparatus to perform at least the following:

receive input; *(See, e.g.,* Specification ¶¶ [0014], [0085], [0105])

detect, notify, and restrict the execution of an application; (*See, e.g.*, Specification ¶¶

[0014], [0085], [0106])

notify the execution of said application to a surveillance center connected to said

communication network by sending a message indicating that an application has been

started; (*See, e.g.*, Specification ¶¶ [0015], [0086], [0107], [0121-0124])

restrict the execution of said application in accordance with a predetermined functional

limit; (*See, e.g.*, Specification ¶¶ [0016], [0088], [0106], [0121])

determine whether the message has been sent; and (*See, e.g.*, Specification ¶¶ [0045-

0049], [0052], [0087], [0125-0126])

further restrict the execution of said application, within a more restrictive functional limit,

based on the determination. (*See, e.g.*, Specification ¶¶ [0050-0053], [0127])

Independent claim 37 recites:

37. An apparatus comprising:

at least one processor; and

at least one memory including computer program code,

the at least one memory and the computer program code configured to, with the at least one

processor, cause the apparatus to perform at least the following:

receive messages comprising application execution related data from a mobile

terminal device, wherein each message of the messages indicates that an

application has been started, and wherein the message is initiated after a

predetermined period of time has passed since the application was first started or

after a predetermined number of input actions has been input to the application;

and (*See, e.g.,* Specification ¶¶ [0012], [0015], [0019], [0026], [0030-0032], [0072], [0086], [0093], [0117])

generate an authorization for a restricted execution of said application within a predetermined functional limit on said mobile terminal, (*See, e.g.,* Specification ¶¶ [0026], [0058], [0072], [0075], [0093], [0101], [0118-0119])

determine to send said generated authorization as a message via said communication network to said mobile terminal device. (*See, e.g.,* Specification ¶¶ [0026], [0058], [0072], [0094], [0101], [0120])

Independent claim 39 recites:

39. Application execution system comprising:

a mobile terminal device comprising:

at least one processor; and

at least one memory including computer program code,

the at least one program code configured to, with the at least one processor, cause the apparatus to perform at least the following:

receive input; (*See, e.g.,* Specification ¶¶ [0014], [0085], [0105])

detect, notify and restrict the execution of an application; (*See, e.g.,* Specification ¶¶ [0014], [0085], [0106])

notify the execution of said application to a surveillance center connected to a communication network by sending a message indicating that an application has been started, (*See, e.g.,* Specification ¶¶ [0015], [0086], [0107], [0121-0124])

restrict the execution of said application in accordance with a predetermined functional

limit; (*See, e.g.*, Specification ¶¶ [0016], [0088], [0106], [0121])

determine whether the message has been sent; and (*See, e.g.*, Specification ¶¶ [0045-

0049], [0052], [0087], [0125-0126])

further restrict the execution of said application, within a more restrictive functional limit,

based on said determination; and (*See, e.g.*, Specification ¶¶ [0050-0053], [0127])

a surveillance center comprising:

an interface to a mobile communication network for receiving messages comprising

application execution related data from a mobile terminal device; and (*See, e.g.*,

Specification ¶¶ [0012], [0015], [0019], [0026], [0030-0032], [0072], [0086], [0093],

[0117])

an authorization generation circuit connected to said interface for generating an

authorization for a restricted execution of said application within predetermined limits

on said mobile terminal, (*See, e.g.*, Specification ¶¶ [0026], [0058], [0072], [0075],

[0093], [0101], [0118-0119])

wherein said interface is configured to send said generated authorization as a message via

said communication network to said mobile terminal device. (*See, e.g.*, Specification

¶¶ [0026], [0058], [0072], [0094], [0101], [0120])

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A.   The rejection of claims 1, 2, 4, 5, 7-9, 15, 16, 20, 22, 23, 25-33 and 36-43 under 35 U.S.C. § 102(b) as being anticipated by *Coley et al.* (US Pub. No. 2001/0011253 A1).

B.   The rejection of claims 3 and 34 under 35 U.S.C. § 103(a) as being unpatentable over *Coley*, as applied to claim 1, in view of *Kolkowski* (WIPO Pub. No. 200249732 A1).

C.   The rejection of claims 10-13 under 35 U.S.C. § 103(a) as being unpatentable over *Coley*, as applied to claim 1, in view of *Raiz et al.* (US Pub. No. 2002/0164025 A1).

D.   The rejection of claims 14 and 35 under 35 U.S.C. § 103(a) as being unpatentable over *Coley*, as applied to claim 1, in view of *Raiz*, and further in view of Applicant Admitted Prior Art ("AAPA").

E.   The rejection of claims 18 and 24 under 35 U.S.C. § 103(a) as being unpatentable over *Coley*, as applied to claim 1, in view of *Meyer* ("TCP Performance Over GPRS," In Proc Wireless communication and Networking Conference, 1999, WCNC, 1999 IEEE, Vol. 3).

F.   The rejection of claim 19 under 35 U.S.C. § 103(a) as being unpatentable over *Coley*, as applied to claim 1.

VII.   ARGUMENT

A.   GROUPING OF CLAIMS

The appealed claims do not stand or fall together. Appellants separately argue the patentability of: (i) independent claims 1, 32 and 39, and their respective dependent claims 2-5, 7-16, 18-20, 22-26, 29-31, 33-36 and 43-44, as Group I; and (b) independent claims 27 and 37, and their respective dependent claims 28, 38 and 40-42, as Group II.

B.   THE GROUP I CLAIMS 1-5, 7-16, 18-20, 22-26, 29-36, 39 AND 43-44 ARE NOT ANTICIPATED BY COLEY

The Examiner bears initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision. *Gilbert & P. Hyatt v. Dudas*, 551 F.3d 1307, 1313 (Fed. Cir. 2008); *In re Glaug*, 283 F.3d 1335 (Fed. Cir. 2002*)*; *In re Rijkaert*, 9 F.3d 1531, 1532 (Fed. Cir. 1992); *In re Oetiker*, 977 F.2d 1992*)*; *In re Piasecki*, 745 F.2d 1468 (Fed. Cir. 1984). To anticipate a patent claim, the identical disclosure in a single reference of each element of a claimed invention, as those elements are set forth in the claims, such that the claimed invention is placed into the recognized possession of one having ordinary skill in the art. *Therasense Inc. v. Becton, Dickinson and Co.*, 593 F3d 1325 (Fed. Cir. 2010); *Praxair, Inc. v. ATMI, Inc.*, 543 F.3d 1308, (Fed. Cir. 2008); *Dayco Prods., Inc. v. Total Containment, Inc.*, 329 F.3d 1358 (Fed. Cir. 2003); *Schering Corp. v. Geneva Pharm.*, 339 F.3d 1373, 1377 (Fed. Cir. 2003), *Crown Operations International Ltd. v. Solutia Inc.*, 289 F.3d 1367 (Fed. Cir. 2002); *Candt Tech Ltd. v. Resco Metal & Plastics Corp.*, 264 F.3d 1344 (Fed. Cir. 2001).

Additionally, "[u]nless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations **arranged or combined in the same way** as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. § 102" (*see*, *Id. Therasense* quoting *Net moneyIN, Inc. v. VeriSign, Inc.*, 535 F.3d 1359 (Fed. Cir. 2008)) (emphasis added).

Although "inherent disclosure" is also a basis of anticipation, (*see, Finnigan Corp. v. Int'l Trade Comm'n*, 180 F.3d 1354, 1365 (Fed. Cir. 1999)), it "does not alter the requirement that all elements must be disclosed in an anticipatory reference in the same way they are arranged or combined in the claim" (*see, Id. Therasense*). "'[A]nticipation by inherent disclosure is appropriate only when the reference discloses prior art that must necessarily include the unstated

limitation.'" (see, *Id.* quoting *Transclean Corp. v. Bridgewood Servs., Inc.*, 290 F.3d 1364, 1373 (Fed. Cir. 2002)). "'Inherency, however, **may not be established by probabilities or possibilities**. The mere fact that a certain thing may result from a given set of circumstances is not sufficient'" *(see, Id.* quoting *In re Oelrich*, 666 F.ed 578, 581 (CCPA 1981)) (emphasis added).

Independent claims 1, 32 and 39 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by *Coley*. Independent claim 1, for example, recites, *inter alia*, the features of "starting a restricted execution of said application, within a predetermined functional limit, after said message has been initiated, determining whether the message has been sent, and further restricting the execution of said application, within a more restrictive functional limit, based on said determination." These features occur where a mobile terminal device has detected an input directed to start execution of an application on the device, and has initiated a message to a surveillance center indicating that the application has been started. Independent claims 32 and 39 recite similar features. Appellants submit that *Coley* fails to disclose or suggest such features as claimed in the present application.

Generally, *Coley* provides a system for automatically tracking software use, determining whether the software is validly licensed and enabling or disabling the software accordingly. (*Coley*, Abstract, ¶¶ 42, 46) A licensing system module forms a license record inquiry message to enable or validate a license to a software application. (*Coley*, Abstract, ¶¶ 42, 47) Records of valid licenses are stored in a database maintained by the software provider, and the licensing system module transmits the license record inquiry to the database server over a public network. (*Coley*, Abstract, ¶¶ 42, 47) In response to the inquiry, the database server determines whether a valid license record exists in the database for the software application. (*Coley*, Abstract, ¶¶ 42,

47) The database server forms and returns an appropriate response message that is interpreted by the licensing system module, and the licensing system module then enables or disables the software application accordingly. (*Coley*, Abstract, ¶¶ 43-44, 47-48)

The Examiner, in the Final Office Action, contends that such features are disclosed in *Coley*. Specifically, according to the statement of the rejection the Examiner asserts as follows:

> Re claim 1, Coley discloses a method comprising:
> …
> starting a restricted execution of said application within a predetermined functional limit, after said message has been initiated (paragraph [79], the Check In License procedure can be used to return a license or disable a feature (predetermined functional limit) when the user has completed use of the client application or the feature contained therein)
> determining whether the message has been sent (paragraph [88], a status message indicating an error code, an indication that the server or agent is presently too busy to handle a query (message has been sent), an indication of a connection or communication failure (message has been sent); paragraph [47], The response message is returned to the client (message has been sent))
> further restricting the execution of said application, within a more restrictive functional limit based on said determination (paragraph [79], the Check In License procedure can be used to return a license or disable a feature (more restrictive functional limit) when the user has completed use of the client application or the feature contained therein. This is clearly based on the determination that a message is sent (paragraph [47], response message to the client module; alternatively see paragraph [92], where Coley teaches that on returning of a null license 10 the client application is disabled. Coley further teaches in paragraph [73], that the client data structure contains the authorization and license 10, and in paragraph [88] that a authorization 10 indicating a failed delivery is return. This implies that when a authorization 10 status of failed delivery is returned through the client data structure, the license 10 is null, since clearly it has not been given a failure, and as such, paragraph [92] necessitates the disabling of the application (further restricting based on the determination of message sent)). (*Final Office Action*, Pp. 4-5)

The Examiner's assertions, however, represent nothing more than a surgical dissection of the teaching of *Coley*, taking individual statements out of context and piecing them together to recreate the present claims. The arguments put forth in the Final Office Action accordingly do <u>not</u> establish that *Coley* discloses each element of the claimed invention, as recited in the claims,

such that the claimed invention is placed into the recognized possession of one having ordinary skill in the art.

The Examiner first asserts that, at Paragraph 79 (with respect to the "Check In License" procedure), *Coley* discloses starting a restricted execution of said application within a predetermined functional limit, after said message has been initiated. According to *Coley*, the Check In License procedure is one of three license validation procedures provided by an exemplary embodiment of the *Coley* disclosure, namely the Check Out License, Validate License, and Check In License. (*Coley*, ¶ 68) The Check Out License procedure is responsible for the initial enablement of a software application, the Validate License procedure is used for periodic re-enablement of a software application, and the "Check In License can be used for decrementing a floating license count, or <u>indicating client application status in a database license record</u> when use of a client application is completed." Accordingly, as an initial matter, Appellants note that the Check In License procedure is used to update the license status in the respective license database record – hence the use of the term Check In (used to input status change in the database record). (*See Coley*, ¶¶ 79-80).

Next, an examination of Paragraphs 79-80 of *Coley* further reveals the Examiner's misinterpretation of the Check In License procedure. As correctly noted by the Examiner, the Check In License procedure can be used to disable the application or a feature of the application when a user has completed use of the application or the particular feature. (*Coley*, ¶ 79) According to the procedure, a new client data structure is first created, including the name of the software application, identification of any features to be disabled, identification of the upstream license agent/server, the license ID and the authorization ID for the software application, etc. (*Coley*, ¶ 79) The license ID provides a pointer designating the location of the respective license

record in the license database of the upstream licensing server. (*Coley*, ¶87) The authorization ID provides the status of a license in response to an enablement (Check Out License) inquiry or validation (Validate License) inquiry, or provides an acknowledgement to a Check In License procedure that permits a client application to delete a client data structure. (*Coley*, ¶ 88)

In accordance with the Check In License procedure, a license check in request message is then sent to the upstream agent, containing the new client data structure, and the license ID information is used by the upstream agent to directly access the database location of the respective license record. (*Coley*, ¶ 80) Based on the client data structure, the existing license record is modified to indicate the disablement of a feature, or is deleted (in the event where the use of a client application is completed). (*Coley*, ¶ 80) The license ID and authorization ID fields of the client data structure are nulled, and a license check in response message containing the client data structure (with the nulled ID's) is then formed by the agent and returned to the client module. (*Coley*, ¶ 80) The client module then deletes the client data structure. (*Coley*, ¶ 80) In other words, according to the Check In License procedure, *Coley* discloses that the respective database license record at the licensing server is either modified or deleted in response to the license check in request sent by the client device, and <u>not</u> (as characterized by the Examiner) that a restricted execution of a client application is started within a predetermined functional limit, after initiation of a message to a surveillance center indicating that the application has been started, as presently claimed.

Appellants further submit that, in the context of the License Check Out and Validate License procedures, *Coley* also fails to disclose the feature of starting a restricted execution of a client application within a predetermined functional limit, after initiation of a message to a surveillance center indicating that the application has been started, as presently claimed.

According to the Check Out License procedure, *Coley* discloses that, when a client application is started, the Check Out License procedure is initiated to enable the software application. (*Coley*, ¶ 70) A client data structure is first created, including the name of the software application, identification of any features to be enabled, identification of the upstream license agent/server, etc. (in this case, because this is an initial validation, the license ID and the authorization ID for the software application will be inserted by the licensing agent). (*Coley*, ¶ 70) The client device then sends a license validity inquiry request message to the upstream agent, including the client data structure, and the licensing agent uses the information from the client data structure to query the database to determine the existence, if any, of a license record for the client application. (*Coley*, ¶ 71)

If the query locates a corresponding license record in the database, a pointer for the record an authorization ID are generated and inserted in the client data structure, and, if the query fails to locate a license record, the license ID and authorization ID fields are left blank or nulled. (*Coley*, ¶ 72) A license validity response message is then sent to the client device, including the license ID and authorization ID, if any. (*Coley*, ¶ 72) The client module examines the license ID and authorization ID fields of the client data structure to determine the license status of the client application. (*Coley*, ¶ 73) If the fields indicate the presence of a valid license, the client device enables the software application, and, if the license ID and authorization ID fields are null, the client device does not enable the software application and deletes the client data structure. (*Coley*, ¶ 73) Similarly, according to the Validate License procedure, *Coley* discloses a process whereby, once a software application has been validated, the client device periodically sends license validity inquiry request messages to the upstream agent to verify that the application is

still validly licensed, and either permits continued execution of the application or disables it based on the status response messages received from the licensing agent. (*See Coley*, ¶¶ 76-78).

Accordingly, with respect to the Check Out License and Validate License procedures, *Coley* discloses that a client device either enables or disables a software application based on a license status message received from a license agent or server, and <u>not</u> the starting a restricted execution of a client application within a predetermined functional limit, as presently claimed. Moreover, *Coley* accordingly discloses that the client device enables or disables the software application only after sending a license validity inquiry request message to the licensing agent, and receives a status message in response thereto, and <u>not</u> that a restricted execution of the client application is started after initiation of the message to the surveillance center, as presently claimed.

Additionally, according to the statement of the rejection set forth in the Office Action, the Examiner further asserts that *Coley* discloses the features of determining whether the message has been sent (citing to Paragraph 88 of *Coley*), and further restricting the execution of said application, within a more restrictive functional limit based on said determination (citing to Paragraph 79 of *Coley*). (*See Office Action*, P. 5, lines 10-19) First, with reference to Paragraph 88, *Coley* discloses various example uses for the authorization ID, one of which being use for "return[ing] a status message containing an error code, an indication that the server or agent is presently too busy to handle a query, an indication of a connection or communication failure, or any other like message." (*Coley*, ¶ 88) With respect to this use of the authorization ID for providing an error message regarding the status of the transmission of a license inquiry request message to the upstream agent, however, *Coley* certainly does <u>not</u> disclose or suggest that the client device further restricts the execution of the application, within a more restrictive functional

limit based on the determination as to whether the license inquiry message has been sent. Indeed, Appellants submit that *Coley* lacks any disclosure or suggestion whatsoever as to any subsequent actions of the client device based on the error message.

Instead, the Final Office Action cites to various other discrete statements from the *Coley* reference, takes these statements out of context, and pieces them together to form an interpretation that is not supported by the *Coley* disclosure. For example, the rejection cites to Paragraph 79 of *Coley* as disclosing the further restriction of the execution of the application based on the determination as to whether the inquiry message has been sent. (*See Office Action*, P. 5, lines 14-19) As presented above, however, Paragraph 79 addresses the Check In License procedure, whereby the license database record at the licensing server is updated to, for example, disable a feature of the client application. (*Coley*, ¶ 79) Further, the Office Action asserts that, because the actions of the client device are based on the response message from the licensing server, the actions are necessarily based on a determination as to whether the inquiry message has been sent. (*See Office Action*, P. 5, lines 19-22) This is clearly not so – one of skill in the art would plainly understand that basing the actions of the client device on a determination as to whether the inquiry message has been sent has nothing to do with the response message – the actions of client device can be determined irrespective of the content of the response message, or whether a response message has even been received. Lastly, the rejection again refers to Paragraph 88 of *Coley*, asserting that an error message in the authorization ID field (with respect to a failure in the transmission of the license inquiry request) infers that the client device would necessarily disable the software application (in accordance with the disclosure of Paragraph 92). (*See Office Action*, P. 6, lines 2-7) However, with respect to Paragraph 88 (and the entire *Coley* disclosure), as presented above, *Coley* lacks any such disclosure or inference regarding the

process of the client device for handling a transmission error message, and, with respect to Paragraph 92, the disclosure regarding disabling a client application is in the context of a validation check, and bears no express or implied relation to a response to a transmission error message.

Finally, in the Response to Arguments section of the Final Office Action, with reference again to Paragraph 79 of *Coley*, the Examiner advances the argument that a subsequent initiation of the application may result in a further restricted execution of the application based on a feature disable through the Check In License procedure (that is, after a prior execution of the application already resulted in an initial disabled feature based on a prior execution of the Check In License procedure). (*See Office Action*, P. 2, Response to Arguments, ¶ 4) In other words, the Examiner's assertion provides that after two different features are disabled, based on two different executions of the Check In License procedure, the client application is started again under a further restricted execution, based on the response message received from the licensing agent. Accordingly, in the context of the present claims, the Examiner is asserting that *Coley* discloses that (after a first execution of the Check In License process disabling a feature of the application) the client device starts the application and initiates a first request message to the licensing server, and, based on the associated response message, the device starts a restricted execution of the application within a predetermined functional limit. Then, (after a second execution of the Check In License process disabling an additional feature) the client device restarts the application and initiates a second request message to the licensing server, and, based on the associated response message, the device starts a further restricted execution of the application. Even under this interpretation, it is clearly evident that *Coley* does not disclose the

feature of further restricting the execution of the application based on a determination as to whether the message has been sent, as presently claimed.

Appellants, therefore, respectfully submit that *Coley* fails to disclose the features of starting a restricted execution of a software application on a mobile device, within a predetermined functional limit, after initiation of a message to a surveillance center indicating that the software application has been started, and further restricting the execution of the application based on a determination as to whether the message has been sent, in the manner as presently claimed.

In light of the foregoing, Appellants submit that *Coley* fails to disclose or suggest the recitations of independent claims 1, 32 and 39 and that, therefore, the rejection of these claims as being anticipated by *Coley* is neither legally nor factually viable. Accordingly, the rejection of these claims under 35 U.S.C. § 102(b) is erroneous and should be reversed. Appellants further submit that, at least by virtue of their dependency from their respective independent claims 1, 32 and 39, claims 2-5, 7-16, 18-20, 22-26, 29-31, 33-36 and 43-44 are not anticipated by *Coley*, and that, for at least the above reasons, the rejection of these claims under 35 U.S.C. § 102(b) is erroneous and should also be reversed.

C.   THE GROUP II CLAIMS 27, 28, 37, 38 AND 40-42 ARE NOT ANTICIPATED BY *COLEY*

Independent claims 27 and 37 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by *Coley*. Independent claim 27, for example, recites, *inter alia*, the features of "receiving a message from a mobile terminal device at a surveillance center, said message comprising application execution related data, wherein the message indicates that the application has been started, and wherein the message is initiated after a predetermined period of time has

passed since the application was first started or after a predetermined number of input actions has

been input to the application." Independent claim 37 recites similar features. Appellants submit

that *Coley* fails to disclose or suggest such features as claimed in the present application.

As the basis for the § 102(b) rejection of claims 27 and 37, the Final Office Action asserts

that "Re claim 27, the claim is the receiving side of the method claim 7 and 44 and would

necessitate the method of claims 7 and 44 be carried out for it to actualize," and therefore rejects

claims 27 and 37 for the same reasons as claims 7 and 44. (*Office Action*, P. 9, lines 12-14) With

respect to claim 44, the Final Office Action asserts that *Coley* discloses "Re claim 44, Coley

discloses wherein the message is initiated after a predetermined period of time has passed since

the application was first started or after a predetermined number of input actions has been input to

the application (paragraph [92], the software license can also be validated in response to the

expiration of a timer)" (*Office Action*, P. 11, lines 13-17) According to Paragraph 92, however,

Coley addresses the frequency of license validation checks, disclosing that software license can

be triggered in response to the expiration of a timer (i.e., periodic validation). (*Coley*, ¶ 92)

Coley further addresses periodic license validation checks at Paragraph 50, disclosing that:

> periodic checks performed at timer expiration, or upon appropriate interrupt,
> use the license ID, which is a pointer, to directly access the database record
> corresponding to the license. **If the license record is found, a response**
> **message indicates so, the software remains enabled, and the timer is reset.**
> **If the record is found empty, it may indicate that the license has expired.**
> **The response message will indicate this, and the software can be disabled.**
> Alternatively, the user may be requested to renew the license within a certain
> period of time before the software application 102 is disabled. (*Coley*, ¶
> 50)(*emphasis added*)

In other words, license validation checks can be initiated periodically after the software

application is already running, and has been initially enabled, for example, through a Check Out

License process. Accordingly, as a result of the response message received in response to a

periodic license validation check, the software either remains enabled/executing or is disabled/halted.   (*See also, Coley*, ¶¶ 76-78, regarding the Validate License procedure) Therefore, while *Coley* discloses that the license validation request message may be sent after a predetermined period of time since the client application was first started, the message indicates that the software application remains running at the client device – and does <u>not</u> provide an indication that the client application is first being started.

Appellants, therefore, respectfully submit that *Coley* fails to disclose the features of receiving, at a surveillance center, a message from a mobile terminal device comprising application execution related data, wherein the message indicates that the application has been started, and is initiated after a predetermined period of time has passed since the application was first started or after a predetermined number of input actions has been input to the application, in the manner as presently claimed.

In light of the foregoing, Appellants submit that *Coley* fails to disclose or suggest the recitations of independent claims 27 and 37 and that, therefore, the rejection of these claims as being anticipated by *Coley* is neither legally nor factually viable. Accordingly, the rejection of these claims under 35 U.S.C. § 102(b) is erroneous and should be reversed. Appellants further submit that, at least by virtue of their dependency from their respective independent claims 27 and 37, claims 28, 38 and 40-42 are not anticipated by *Coley*, and that, for at least the above reasons, the rejection of these claims under 35 U.S.C. § 102(b) is erroneous and should also be reversed.

D.   CLAIMS 3 AND 34 ARE NOT RENDERED OBVIOUS BY *COLEY*, AS APPLIED TO CLAIM 1, IN VIEW OF *KOLKOWSKI*

The Final Office Action cites to *Kolkowski* for the alleged disclosure of surveyed executing of an application on a mobile terminal device, where the application is a game. Applicants submit, however, that *Kolkowski* does not provide for the foregoing deficiencies of *Coley*, as presented in subsection B, above.

Accordingly, no *prima facie* case of obviousness has been established with regard to claims 3 and 34, and that, therefore, the rejection of these claims under 35 U.S.C. § 103(a) is neither legally or factually viable and should be reversed.

E.   CLAIMS 10-13 ARE NOT RENDERED OBVIOUS BY *COLEY*, AS APPLIED TO CLAIM 1, IN VIEW OF *RAIZ*

The Final Office Action cites to *Raiz* for the alleged disclosure of certain elements of claims 10-13, which are admitted by the Examiner as lacking from *Coley*. Applicants submit, however, that *Raiz* does not provide for the foregoing deficiencies of *Coley*, as presented in subsection B, above.

Accordingly, no *prima facie* case of obviousness has been established with regard to claims 3 and 34, and that, therefore, the rejection of these claims under 35 U.S.C. § 103(a) is neither legally or factually viable and should be reversed.

F.   CLAIMS 14 AND 35 ARE NOT RENDERED OBVIOUS BY *COLEY*, AS APPLIED TO CLAIM 1, IN VIEW OF *RAIZ*, AS APPLIED TO CLAIM 11, AND FURTHER IN VIEW OF THE ALLEGED APPLICANT ADMITTED PRIOR ART (AAPA)

The Final Office Action cites to the alleged AAPA for the alleged disclosure of the payment transaction being charged to the next telephone bill. Applicants submit, however, that

the alleged AAPA does not provide for the foregoing deficiencies of *Coley*, as presented in subsection B, above.

Accordingly, no *prima facie* case of obviousness has been established with regard to claims 3 and 34, and that, therefore, the rejection of these claims under 35 U.S.C. § 103(a) is neither legally or factually viable and should be reversed.

G.   CLAIMS 18 AND 24 ARE NOT RENDERED OBVIOUS BY *COLEY*, AS APPLIED TO CLAIM 1, IN VIEW OF *MEYER*,

The Final Office Action cites to *Meyer* for the alleged disclosure of a TCP system used in a mobile terminal device, wherein the message is determined as not being sent, if a confirmation message that said message has been sent is not received within a defined period, and the message being sent via a general packet radio service. Applicants submit, however, that *Meyer* does not provide for the foregoing deficiencies of *Coley*, as presented in subsection B, above.

Accordingly, no *prima facie* case of obviousness has been established with regard to claims 18 and 24, and that, therefore, the rejection of these claims under 35 U.S.C. § 103(a) is neither legally or factually viable and should be reversed.

H.   CLAIM 19 IS NOT RENDERED OBVIOUS BY *COLEY*, AS APPLIED TO CLAIM 1

The Final Office Action takes official notice that, at the time the invention was made, buffering of messages not sent was known and expected when a TCP mechanism was used in communication. Applicants submit, however, that the subject matter of the official notice does not provide for the foregoing deficiencies of *Coley*, as presented in subsection B, above.

Accordingly, no *prima facie* case of obviousness has been established with regard to claims 18 and 24, and that, therefore, the rejection of these claims under 35 U.S.C. § 103(a) is neither legally or factually viable and should be reversed.

VIII. CONCLUSION AND PRAYER FOR RELIEF

Based on the foregoing, it is apparent that none of the rejections under 35 U.S.C. §§ 102(b) and 103(a) is factually or legally viable. Appellants therefore solicit the Honorable Board to reverse each of the Examiner's rejections.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 504213 and please credit any excess fees to such deposit account.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

February 15, 2011   /Phouphanomketh Ditthavong/
Date   Phouphanomketh Ditthavong
                                   Attorney for Applicant(s)
                                   Reg. No. 44658

                                   Craig Plastrik
                                   Attorney/Agent for Applicant(s)
                                   Reg. No. 41254

918 Prince Street
Alexandria, VA 22314
Tel. (703) 519-9952
Fax (703) 519-9958

IX.   CLAIMS APPENDIX

1. Method comprising:

detecting, at a mobile terminal device, an input directed to start execution of an application on

said mobile terminal device;

initiating a message to a surveillance center, wherein said message indicates that the

application has been started;

starting a restricted execution of said application, within a predetermined functional limit,

after said message has been initiated;

determining whether the message has been sent; and

further restricting the execution of said application, within a more restrictive functional limit,

based on said determination.

2. Method according to claim 1, further comprising:

determining to send said message to said surveillance center; and

starting said restricted execution of said application, within the predetermined functional

limit, after said message has been sent.

3. Method according to claim 1, wherein said application is a game application.

4. Method according to claim 1, wherein said message indicates the start of an execution of

an application.

5. Method according to claim 1, wherein said restricted execution is further based on a time

limit.

6. (Canceled)

7. Method according to claim 1, wherein said initiating of a message to said surveillance center comprises:

setting up a connection to the surveillance center;

determining to send the message to the surveillance center, said message comprising application execution related data; and

receiving an authorization to execute said application within said limits defined by said surveillance center.

8. Method according to claim 7, wherein said application execution related data comprise:

data from an application identification, mobile electronic terminal identification, user identification, player identification, communication parameter, pin-code, or a combination thereof.

9. Method according to claim 1, wherein said application determines to send said message to said surveillance center.

10. Method according to claim 7, further comprising:

determining to output a user-authorization request to send the message to the surveillance center; and

detecting a user-authorization input authorizing said connection set up.

11. Method according to claim 1, further comprising:

determining to output a user-authorization request to perform a payment transaction;

detecting a user-authorization input for authorizing said payment transaction, and

performing said authorized payment transaction.

12. Method according to claim 11, wherein said authorized payment transaction is performed by charging an onboard payment device.

13. Method according to claim 11, wherein said authorized payment transaction is performed by sending said authorization for said payment transaction to said surveillance center.

14. Method according to claim 11, wherein said payment transaction is charged to the next telephone bill.

15. Method according to claim 1, wherein said message is sent periodically.

16. Method according to claim 1, wherein said application determines the number of messages to be sent and the point in time a message is sent.

17. (Canceled)

18. Method according to claim 1, wherein said message is determined as not being sent, if a confirmation message that said message has been sent is not received within a defined period.

19. Method according to claim 1, further comprising:

buffering of said messages not sent.

20. Method according to claim 1, further comprising:

determining conditions that prevent the sending of said message, wherein the execution of

    said application is further based on whether the conditions are present.

21. (Canceled)

22. Method according to claim 1, further comprising:

receiving a confirmation message that said message has been sent.

23. Method according to claim 1, further comprising:

interrupting the execution of said application, if said message has not been sent.

24. Method according to claim 1, wherein said message is sent via general packet radio service.

25. Method according to claim 1, further comprising downloading application software to said mobile terminal device.

26. Method according to claim 1, further comprising:

comparing a time rule provided in said application with an actual date; and

interrupting the execution of said application, if said actual date does not meet said time rule.

27. Method comprising:

receiving a message from a mobile terminal device at a surveillance center, said message comprising application execution related data, wherein the message indicates that the application has been started, and wherein the message is initiated after a predetermined period of time has passed since the application was first started or after a predetermined number of input actions has been input to the application;

generating, at the surveillance center, an authorization to a restricted execution of said application within predetermined functional limits on said mobile terminal device; and

determining to send said authorization to said mobile terminal device.

28. Method according to claim 27, further comprising:

evaluating said message received from said mobile terminal device at a surveillance center;

determining to store a result of said evaluation and an identification related to the use of said

application in said data base; and

generating said authorization to a restricted execution of said application in accordance with

said result of said evaluation.

29. Method for enabling the surveyed execution of an application on said mobile terminal

device, by using a data exchange with a surveillance center, comprising the steps of claim 1.

30. Software tool comprising program code means stored on a non-transitory computer

readable storage medium for carrying out the method of claim 1 when said software tool is run on

a computer or network device.

31. Computer program product comprising program code means stored on a non-transitory

computer readable storage medium for carrying out the method of claim 1 when said program

product is run on a computer or network device.

32. An apparatus comprising:

at least one processor; and

at least one memory including computer program code,

the at least one program code configured to, with the at least one processor, cause the

apparatus to perform at least the following:

receive input;

detect, notify, and restrict the execution of an application; notify the execution of said

application to a surveillance center connected to said communication network by

sending a message indicating that an application has been started;

restrict the execution of said application in accordance with a predetermined functional

limit;

determine whether the message has been sent; and

further restrict the execution of said application, within a more restrictive functional limit,

based on the determination.

33.   An apparatus according to claim 32, wherein said apparatus is further caused to receive

authorizations from said surveillance center, comprising said limits for executing said

application, and restrict the execution of said application on said processing unit in accordance

with said limits.

34. An apparatus according to claim 32, wherein said apparatus is a game device.

35.   An apparatus according to claim 32, wherein said apparatus comprises a cellular

telephone.

36. An apparatus according to claim 32 further comprising a buffer for messages, said buffer

is capable to buffer messages, wherein the apparatus is further cased to:

buffer the message based on the determination, wherein the execution of said application is

further based on whether said buffer is full.

37. An apparatus comprising:

at least one processor; and

at least one memory including computer program code,

the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform at least the following:

receive messages comprising application execution related data from a mobile terminal device, wherein each message of the messages indicates that an application has been started, and wherein the message is initiated after a predetermined period of time has passed since the application was first started or after a predetermined number of input actions has been input to the application; and

generate an authorization for a restricted execution of said application within a predetermined functional limit on said mobile terminal,

determine to send said generated authorization as a message via said communication network to said mobile terminal device.

38. An apparatus according to claim 37, said apparatus is further caused to:

evaluate messages received from said mobile terminal device, via an interface,

determine to store a result of said evaluation and an identification related to the use of said application in an evaluation circuit, and

generate said authorization to a restricted execution of said application in accordance with a result received from said evaluation circuit.

39. Application execution system comprising:

a mobile terminal device comprising:

at least one processor; and

at least one memory including computer program code,

the at least one program code configured to, with the at least one processor, cause the apparatus to perform at least the following:

receive input;

detect, notify and restrict the execution of an application;

notify the execution of said application to a surveillance center connected to a communication network by sending a message indicating that an application has been started,

restrict the execution of said application in accordance with a predetermined functional limit;

determine whether the message has been sent; and

further restrict the execution of said application, within a more restrictive functional limit, based on said determination; and

a surveillance center comprising:

an interface to a mobile communication network for receiving messages comprising application execution related data from a mobile terminal device; and

an authorization generation circuit connected to said interface for generating an authorization for a restricted execution of said application within predetermined limits on said mobile terminal,

wherein said interface is configured to send said generated authorization as a message via said communication network to said mobile terminal device.

40.   Method for enabling the surveyed execution of an application on said mobile terminal device, by using a data exchange with a surveillance center, comprising the steps of claim 27.

41.   Software tool comprising program code means stored on a non-transitory computer readable storage medium for carrying out the method of claim 27 when said software tool is run on a computer or network device.

42.   Computer program product comprising program code means stored on a non-transitory computer readable storage medium for carrying out the method of claim 27 when said program product is run on a computer or network device.

43.   Method according to claim 1, further comprising:

buffering the message based on the determination, wherein the execution of said application
       is further based on whether said buffer is full.

44.   Method according to claim 1, wherein the message is initiated after a predetermined period of time has passed since the application was first started or after a predetermined number of input actions has been input to the application.

X. <u>EVIDENCE APPENDIX</u>

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI.   RELATED PROCEEDINGS APPENDIX

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.